REMARKS:

Claims 1-51 are pending. Claims 1-26, 30-33, 36-37, 39, 41, 43-46, and 49-50 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,256,737 to Bianco et al. Claims 27-29 and 34 are rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,256,737 to Bianco et al. Claims 35 and 48 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al in view of U.S. Patent No. 6,233,618 to Herz. Claims 38 and 51 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al in view of U.S. Patent No. 6,233,618 to Shannon. Claim 40 is rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al in view of U.S. Patent No. 6,011,858 to Stock et al. Claims 42 and 47 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al in view of U.S. Patent No. 6,119,096 to Mann et al.

Reconsideration is requested. No new matter is added. The specification has been amended as requested by the Examiner. Claims 1, 20, and 25 are amended to clarify the invention. Claims 34 and 47 are amended to correct typographical errors. The rejections are traversed. Claims 1-51 remain in the case for consideration.

Rejections under 35 U.S.C. § 102(e):

Referring to claim 1, the instant invention is directed toward a method for processing electronic transactions. A user registers with an electronic identicator a registration biometric sample. The user formulates a rule module in a clearinghouse. The rule includes at least one pattern data and at least one execution command. The user is then identified by comparing a bid biometric sample against the biometric samples registered in the electronic identicator. Assuming the user is identified, a rule module of the user is invoked, to execute at least one electronic transmission.

Referring to claim 20, the instant invention is a system for processing electronic transactions. A biometric input apparatus is used, for providing a registration biometric sample to an electronic identicator during registration, and for providing a bid biometric sample to the electronic identicator when the user wants to execute an electronic transmission. A clearinghouse stores rule modules, combining pattern data with execution commands. An execution module invokes an execution command from a rule module, responsive to the electronic identicator indicating whether the user is successfully identified.

Referring to claim 25, the instant invention is a method for processing electronic transactions. Two users, a primary and a subordinate, each register biometric samples with an electronic identicator. The users also formulate rule modules, associating pattern data with execution commands. The subordinated user is then identified by the electronic identicator. Assuming the subordinated user is successfully identified, the subordinated user's rule modules are checked to see if they are subordinated to any of the primary user's rule modules. Assuming that one of the subordinated user's rule modules are subordinated to one of the primary user's rule modules, the primary user's rule modules are invoked, thereby executing an electronic transmission.

In contrast, Bianco teaches a system for authenticating users and granting conditional access to resources. In Bianco, the user provides a user ID. The biometric group to which the user belongs is determined, its biometric policy controlling the authentication of the user. The user's registered biometric sample, associated with the user ID, is also determined. The user's biometric sample is compared with the registered sample. If the samples match per the biometric policy, then the resources associated with the biometric group may be accessed by the user.

There are two key differences between the instant invention as defined in claims 1, 20, and 25, and the Bianco patent. These are how the methods and systems compare the user's biometric sample with the registered biometric sample, and the use of the rule modules.

In reviewing the Bianco patent, it is apparent that the inventors intended to describe the process of "authenticating" a user, while using the technical term "identification" for the operation. The terms "identification" and "authentication" are known in the art, and have very specific meanings. "Identification" is the process of determining the identity of a user, whereas "authentication" is the process of determining if a user is who he says he is. Put another way, "identification" answers the question "Who am I?", whereas "authentication" answers the question "Am I John Doe?". These are very different processes, as will be seen below.

In identifying a user, a key assumption is that the user has made no assertion whatsoever as to his identity. Accordingly, to identify a user, the offered biometric sample has to be compared with *every* registered biometric sample in the database. Once a match is found, the user's identity has been determined.

In contrast, when a user is being authenticated, the user has already made an assertion as to who he is. The question becomes one of confirming or rejecting the assertion. This requires comparing the offered biometric sample with *only one* registered biometric sample: the registered biometric sample associated with the person the user claims to be.

A single comparison, as required to authenticate a user, is a much simpler proposition than the open-ended comparison of a biometric sample with every registered biometric in a database. A single compare takes a relatively short amount of time, whereas the large number of comparisons required to identify a user can take an inordinate amount of time. (Granted, if the user's biometric sample matches the first registered biometric in the database, the identification will have taken a very short amount of time, but on average, the user's biometric sample has to be compared with ½ of the registered samples in the database. Assuming 10 million users (a relatively small database) each registered only three fingers, identifying an individual user requires 15,000,000 comparisons, which take a lengthy amount of time.)

The Examiner referred to column 8, lines 14-21, as support for the proposition that Bianco teaches user identification from biometrics. The Applicant does not dispute that Bianco uses the term "identification" or some variant thereof at many points (e.g., Abstract, column 2, line 67, column 6, lines 36, 39, 48, 50, 54 and 59, column 7, lines 3, 34, 48, 53, 54-55, 56, and 58, and more too numerous to list). But it is nonetheless clear that Bianco intends to describe only authentication. Indeed, even at many of above citations, Bianco uses the term "authentication" or some variant thereof in the same sentence. For example, at column 6, lines 39-40, Bianco explains that the "identification" of the user is "to provide effective authentication to resources."

Although Bianco does not describe the user as asserting his identity in column 8, column 8 is couched in language suggesting that the user has already made some identification to the system. For example, at column 8, lines 16-17, Bianco says that "[t]he live biometric data is matched with the stored biometric data." The "live biometric data" is the biometric sample provided when the user is attempting to authenticate himself, which is compared with the "stored biometric data," provided at the time the user registered with the system. There is no text to suggest that Bianco is doing anything more than the a one-to-one comparison of the biometric sample against the registered sample associated with the user.

Were Bianco doing the more general identification, there sentence would have been written more like "[t]he live biometric data is compared with the stored biometric data to see if the live biometric data matches any stored biometric data." Bianco's treatment of the word "data" as a singular noun (grammatically incorrect, since "data" is a plural noun: "datum" is the singular form) in the context of "live biometric data" suggests that he views "data" to always be a singular noun, and "stored biometric data" must be viewed as a single stored biometric sample.

The view that Bianco is performing mere authentication and not identification is further reinforced later in the patent. At column 23, lines 31-32 (referring to FIG. 8A), the user is described as typing in a user ID. This limits the registered biometric against which the user's biometric sample is compared to a single registered biometric.

Bianco's careless use of the terms "identification" and "authentication" force the reader to review the patent to determine which process is intended. From the fact that Bianco expects the user to provide a user ID before the biometric sample is tendered, the reasonable interpretation is that Bianco is performing only authentication, despite the actual words used. Since identification is not being taught by Bianco, claims 1, 20, and 25 (and all claims dependent from these claims) are allowable over Bianco.

The second difference between the instant invention and Bianco is the rule module. In the instant invention, the rule modules are user-customizable. As stated at page 19, lines 1-2, "'user-customized' [means] hav[ing] been customized by or for a user." In other words, the user has the capability of customizing the rules (either the pattern data or the execution command associated with the pattern data). In addition, rule modules can include more than one of either the pattern data or the execution command. Finally, a user can have more than one rule module, meaning that with a single identification, many different electronic transmissions can be sent, using one or more rule modules. In addition, although the execution commands can enable access to resources, this is but one of a great many different actions that execution commands can achieve.

In contrast, Bianco uses biometric groups to control resource access (and nothing more). Further, resource access is associated with the biometric group. This means two things: the "rules" are not associated with individual users, and the user has no ability to change the "rules" as he likes. Since the user cannot customize the "rules," Bianco does not teach user-customizable rules, as claimed in the instant invention.

Further, Bianco does not teach anything akin to the pattern data of the instant invention. The "rule" granting access to the biometric group resources is automatically invoked once the user is authenticated. There is no conditional execution, comparable to the pattern data of the instant invention.

Finally, because the resources associated with only one biometric group can be accessed at a single time, any "rules" associated with a different biometric group cannot be invoked. Bianco does account for the fact that a user may be a member of more than one biometric group. But as stated at column 23, lines 28-50, Bianco uses the user ID to determine the biometric group the user is in. Since only a single biometric policy can control at any one time, "rules" associated with a different biometric group of which the user is a member cannot be executed, even if the "pattern data" for those rules would be matched.

The invention as defined by claim 1 is directed toward:

> A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:
>
> a. a user registration step, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;
>
> b. formation of a *user-customizable rule module* customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is associated with at least one execution command of the user;
>
> c. a user identification step, wherein the electronic identicator *compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user*;
>
> d. a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission;
>
> wherein a biometrically authorized electronic transmission is conducted without the user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

(claim 1; italics added). As these features are not taught or suggested by Bianco, claim 1 is patentable under 35 U.S.C. § 102(e) over Bianco. Accordingly, claims 1-19 and 26-38 are allowable.

The invention as defined by claim 20 is directed toward:

> A computer system device for tokenless biometric processing of electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, comprising:
>
> a. a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identicator; wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;
>
> b. an electronic rule module clearinghouse, having at least one *user-customizable rule module* further comprising at least one pattern data of the user associated with at least one execution command of the user, for executing at least one electronic transmission;
>
> c. an electronic identicator, for *comparing the bid biometric sample with registered biometric samples of users*;
>
> d. a command execution module, for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission;
>
> wherein no man-made memory tokens such as smartcards, or magnetic swipe cards are presented by the user to conduct the electronic transmission.

(claim 20; italics added). As these features are not taught or suggested by Bianco, claim 20 is patentable under 35 U.S.C. § 102(e) over Bianco. Accordingly, claims 20-24 and 39-51 are allowable.

The invention as defined by claim 25 is directed toward:

> A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:
>
> a. a primary and subordinated user registration step, wherein a primary and subordinated user each register with an electronic identicator at least one registration biometric sample taken directly from the person of the primary and subordinated user, respectively;

b. formation of a rule module customized to the primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the primary and subordinated user is associated with at least one execution command of the primary and subordinated user, *the rule module customized to the primary user is customizable by the primary user and the rule module customized to the subordinated user is customizable by the subordinated user*, and;

c. a subordinated user identification step, wherein the electronic identicator *compares a bid biometric sample taken directly from the person of the subordinated user with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user*;

d. a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules;

e. a command execution step, wherein upon the successful identification of the subordinated user and the determination that at least one of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the primary user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the primary and subordinated user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

(claim 25; italics added). As these features are not taught or suggested by Bianco, claim 25 is patentable under 35 U.S.C. § 102(e) over Bianco. Accordingly, claim 25 is allowable.

Rejections under 35 U.S.C. § 103(a):

The Examiner rejected claims 27-29, 34-35, 38, 40, 42, 47-48, and 51 using various combinations of Bianco and other references. None of the other references teach the combination of identification and user-customizable rule modules. Therefore claims 27-29, 34-35, 38, 40, 42, 47-48, and 51 are all allowable.

For the foregoing reasons, reconsideration and allowance of claims 1-30 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

20575
PATENT TRADEMARK OFFICE

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

By Ariel Rogson
Ariel Rogson
Reg. No. 43,054

1030 S.W. Morrison Street
Portland, Oregon 97205
Telephone: (503) 222-3613

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO:
□ COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON D.C. 20231
☒ ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON D.C. 20231
□ ASSISTANT COMMISSIONER FOR TRADEMARKS, 2900 CRYSTAL DRIVE, ARLINGTON, VA 22202-3513
ON September 23, 2002
Deanna Brusco

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please amend claims 1, 20 and 25 as follows:

1. (First Amendment) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

a. a user registration step, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

b. formation of a user-customizable rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is associated with at least one execution command of the user;

c. a user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user;

d. a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

20. (First Amendment) A computer system device for tokenless biometric processing of electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, comprising:

a. a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identicator; wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

b. an electronic rule module clearinghouse, having at least one user-customizable rule module further comprising at least one pattern data of the user associated with at least one execution command of the user, for executing at least one electronic transmission;

c. an electronic identicator, for comparing the bid biometric sample with registered biometric samples of users;

d. a command execution module, for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission;

wherein no man-made memory tokens such as smartcards, or magnetic swipe cards are presented by the user to conduct the electronic transmission.

25. (First Amendment) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

a. a primary and subordinated user registration step, wherein a primary and subordinated user each register with an electronic identicator at least one registration biometric sample taken directly from the person of the primary and subordinated user, respectively;

b. formation of a rule module customized to the primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the primary and subordinated user is associated with at least one execution command of the primary and subordinated user, the rule module customized to the primary user is customizable by the primary user and the rule module customized to the subordinated user is customizable by the subordinated user, and;

c. a subordinated user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the subordinated user with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user;

d. a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules;

e. a command execution step, wherein upon the successful identification of the subordinated user and the determination that at least one of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the primary user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the primary and subordinated user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

34. (First Amendment) The method of claim 29 wherein the vehicle of travel further comprises any of the following: an airplane; a train; a boat[,] ; and[;] , a bus.

47. (First Amendment) The device of claim 42 wherein the vehicle of travel further comprises any of the following: an airplane; a train; a boat[,] ; and[;] , a bus.

In the specification:

Please replace the paragraph beginning at page 1, line 10 with the following:

This application is a continuation-in-part of US application serial number 09/244,784 filed February 5, 1999, now [pending,] US Patent No. 6,012,039, which is a continuation-in-part of US application serial number [07/705,399,] 08/705,399, filed on August 29, 1996 now US Patent No. 5,870,723, which is a continuation-in-part of US application serial No. 08/442,895 filed on May 17, 1995 now US Patent No. 5,613,012 which is a continuation-in-part of US application serial No. 08/345,523, filed on November 28, 1994, now US Patent No. 5,615,277, all of which are incorporated herein by reference.